SMARTCARD HOLDER'S RESPONSIBILITIES

SMARTCARD HOLDER'S RESPONSIBILITIES

If there are any questions concerning your responsibilities as a smartcard holder, please ask a District Security Officer (dSO) for an explanation. If there are no questions, sign and date this form; make a copy of the signed form for your records and return the original to the issuing dSO.

1. RECEIVING YOUR SMARTCARD.

   a. If a user appears in person to receive a smartcard:

      (1) A valid driver license or Civilian ID card may be required to verify identification.

      (2) The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

      (3) After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

         - If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

         - If the smartcard being issued is for a SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

      (4) The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

      (5) The bottom portion containing the smartcard holder’s unique PIN (i.e., password) is kept by the individual.

   b. If a user is remotely located and cannot receive his/her card in person:

      (1) If the smartcard request is approved by the Smartcard Approver, the dSOs will assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

      (2) The requestor will be mailed the smartcard by **Certified Mail - Return Receipt Requested**.

(3) When you receive the smartcard, sign for the Certified Mail and call the issuing dSO to let him/her know you have received your smartcard. If you do not receive your smartcard in a reasonable amount of time or if the smartcard is damaged, notify the dSO so that appropriate action can be taken.

(4) Upon confirmation that you have the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

(5) When received, sign for the mail. Examine the PIN envelope for tampering. If okay, sign the top portion of the PIN envelope and tear it open. The bottom portion contains your PIN and serial number of your assigned card. **Memorize the PIN and destroy the bottom portion** of the envelope by shredding or burning. Any hard copy of a PIN must be kept in your physical possession or secured in a locked cabinet, drawer, or container accessible only by you.

(6) Return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

(7) Call the issuing dSO to acknowledge receipt of the PIN envelope.

(8) Upon confirmation that you have received the PIN envelope, the appropriate dSO will activate the smartcard.

2. SMARTCARD and PIN USAGE. Your smartcard is logged on when entering CEFMS and logged off with a normal termination. **DO NOT LEAVE THE COMPUTER UNTIL YOU HAVE COMPLETED YOUR SESSION.**

   a. When exiting CEFMS, DO NOT remove your smartcard until you see the message "USER CARD IS BEING LOGGED OFF". Then you may remove your smartcard. If you remove your smartcard prior to this message, it will become locked.

   b. If your smartcard becomes locked, enter the CEFMS database again. A screen will prompt you to insert your smartcard and enter your PIN. If done properly, this procedure will unlock your smartcard, and allow you to successfully log into CEFMS.

3. SECURITY OF THE SMARTCARD AND PIN. Memorize your PIN. DO NOT write it down (especially on the smartcard) or share with others.

   a. When not in use, keep your smartcard in your possession, preferably a wallet or purse, or in a locked cabinet, drawer, or container accessible only by you. DO NOT LEAVE YOUR WALLET OR PURSE UNSECURED OR UNATTENDED BY YOU.

   b. If you retire, transfer, or leave the organization, you must notify the dSOs, return your smartcard to them for deactivation, and sign a Log Sheet for Deactivated Smartcards.

   c. Think of your smartcard as a personal credit card or blank check. The Electronic Signature generated by the smartcard is your signature. If another person uses it, you will bear the consequences.

4. SECURITY OF YOUR SMARTCARD AND PIN. A lost smartcard or compromised PIN is a serious security issue. You can be held responsible for transactions authorized with the missing or compromised card.

   a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a dSO immediately for a new smartcard. Take the smartcard to the dSOs for deactivation and sign the Log Sheet for Deactivated Smartcards. Messages previously "signed" by you may still be verified.

   b. If your smartcard is lost/stolen, contact a dSO immediately for deactivation. You must go to the dSOs to obtain a new smartcard and PIN and sign a Log Sheet for Lost/Stolen Smartcards. Signatures generated by the lost/stolen smartcard after the deactivation date may not be verified.

5. SECURITY VIOLATIONS - WHAT SHOULD YOU REPORT? In addition to the above, report the following to the Security Office.

   a. If you see or know of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

   b. If you find an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

c. If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

d. If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

I certify that I have read and understand my responsibilities as a Smartcard Holder and that I am a Government employee.

PRINTED OR TYPED NAME	**SIGNATURE**

OFFICE SYMBOL	**EXTENSION**	**DATE**